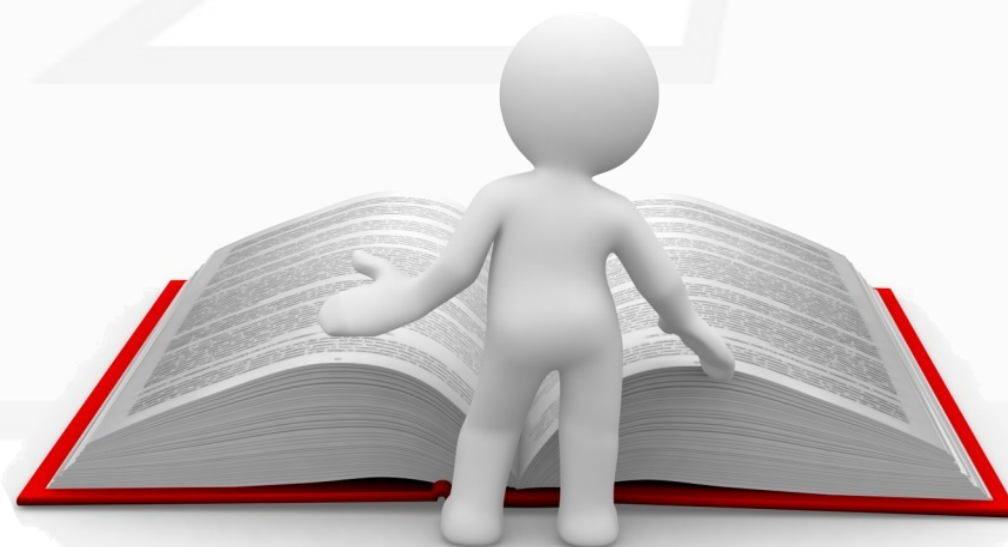
Cursos, soluções e serviços baseados em software livres e padrões abertos para ambientes de missão crítica

Linux Network Servers

OpenVPN

CONCEITO DE VPN

CONCEITO

➔ O que é VPN?

O surgimento da VPN se deve a necessidade de se utilizar redes de comunicação não confiáveis, como a Internet para trafegar informações de forma segura. A Virtual Private Network no passado já esteve associada a serviços remotos de conectividade, como a rede de telefonia pública comutada (RTPC) ou os PVCs (Permanent Virtual Circuits/Channel) do Frame Relay.

A VPN utiliza protocolos de tunelamento e procedimentos de encriptação, garantindo a integridade e autenticidade dos dados. Com a VPN é possível interligar duas ou mais redes, em diferente tipos de sistemas operacionais.

CONFIGURANDO OPENVPN COM CHAVE ESTÁTICA

CONFIGURANDO O SERVIDOR

Nesta configuração, vamos usar chaves estáticas, que é a forma mais simples de configurar a VPN.

Vamos gerar uma chave que será usada tanto pelo servidor quanto pelo cliente.

 # aptitude install openvpn

 # openvpn --genkey --secret /etc/openvpn/chave

CONFIGURANDO O SERVIDOR

 # vim /etc/openvpn/server.conf

```
dev tun
ifconfig 10.0.0.1 10.0.0.2
secret /etc/openvpn/chave
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
```

CONFIGURANDO O SERVIDOR

dev tun → Habilita suporte ao drive TUN/TAP;

ifconfig → Cria o IP do servidor (10.0.0.1) com suporte ao IP do cliente (10.0.0.2);

secret → Comando para chamar nossa chave criptografada e o local dela;

port → Define a porta que a OpenVPN vai rodar;

comp-lzo → Ativa suporte a compressão;

verb → Nível para depuração de erros;

keepalive → Envia um ping a cada 10 segundos sem atividade e a VPN é reiniciada depois de 120 segundos sem respostas.

CONFIGURANDO O SERVIDOR

persist-key → Assegura que o daemon mantenha as chaves carregadas, quando a VPN é restabelecida depois de uma queda de conexão;

persist-tun → Assegura que o daemon mantenha a interface tun aberta, quando a VPN é restabelecida depois de uma queda de conexão;

float → Permite que o túnel continue aberto mesmo que o endereço IP da outra máquina mude.

CONFIGURANDO O CLIENTE

```
# aptitude install openvpn
# vim /etc/openvpn/client.conf
dev tun
ifconfig 10.0.0.2 10.0.0.1
remote 192.168.200.1
secret /etc/openvpn/chave
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
```

INICIANDO O SERVIÇO

Copie o arquivo chave que está em /etc/openvpn/ do Servidor para o /etc/openvpn do cliente.

No servidor:
 # /etc/init.d/openvpn start

No cliente:
 # /etc/init.d/openvpn start

INICIANDO O SERVIÇO

No servidor:

 # ifconfig

tun0 Link encap:Não Especificado Endereço de HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet end.: 10.0.0.1 P-a-P:10.0.0.2

No cliente:

 # ifconfig

tun0 Link encap:Não Especificado Endereço de HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet end.: 10.0.0.2 P-a-P:10.0.0.1

CONFIGURANDO OPENVPN COM CERTIFICADOS

MELHORANDO A SEGURANÇA

A OpenVPN oferece vários mecanismos para adicionar camadas adicionais de segurança, como por exemplo rodar em chroot, uso de conexões TLSs, certificados, uso de chaves com maiores bits. Todas essas camadas previnem ataques como “Man in the Middle”, “DoS”, “Flooding”, “Port scanning” e “Buffer overflow”.

OPENVPN SEM PRIVILÉGIO DE ROOT

Adicione a configuração no servidor e cliente:, as opções “user” e “group” para que o OpenVPN seja executado como usuário nobody e grupo nogroup.

 # vim /etc/openvpn/server.conf
 # vim /etc/openvpn/client.conf

No final do arquivo coloque:
user nobody
group nogroup

Tls-auth HMAC

Você pode adicionar uma assinatura que será verificada antes do processamento de todos os pacotes UDP. Em nossa configuração do servidor vamos habilitar as seguintes opções:

tls-auth → Habilita o controle de conexões tls;
tls-server → Ajuda a bloquear ataques DoS e flooding na porta do OpenVPN;
ca → Certificado de autoridade (CA) que usa as bibliotecas do OpenSSL;
cert → Certificado do servidor;
key → Chave RSA de 2048 do servidor;
dh → Parâmetros Diffie-Hellman utilizado para a troca das chaves criptografadas durante a execução;
cipher → Define um tipo de criptografia maior.

Tls-auth HMAC

Para gerar os certificados e chaves o OpenVPN traz junto a sua instalação, uma série de scripts chamados “easy-rsa”.

Eles podem ser encontrados em **/usr/share/doc/openvpn/examples/easy-rsa/2.0/**

 # ls /usr/share/doc/openvpn/examples/easy-rsa/2.0/

```
build-ca            build-key-server  Makefile                 sign-req
build-dh            build-req         openssl-0.9.6.cnf.gz     vars
build-inter         build-req-pass    openssl.cnf              whichopensslcnf
build-key           clean-all         pkitool
build-key-pass      inherit-inter     README.gz
build-key-pkcs12    list-crl          revoke-full
```

Tls-auth HMAC

Veja que na lista de scripts cada um, tem uma função especifica para criação de certificados e chaves. Vamos copiar o diretório com os scripts para nossa instalação do OpenVPN

 # cp -a /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn/

Acesse o diretório com os scripts copiados:
 # cd /etc/openvpn/2.0

Tls-auth HMAC

Crie o subdiretório onde serão armazenadas as chaves e certificado:

 # mkdir keys

Gerando certificado CA e chave RSA

Utilizando os scripts vamos gerar os certificados e chaves, que serão utilizados em nossa configuração do OpenVPN.

GERANDO CERTIFICADO

Instale o pacote openssl:

```
# aptitude install openssl

# vim vars

export KEY_SIZE=2048
export KEY_COUNTRY="BR"
export KEY_PROVINCE="SP"
export KEY_CITY="SaoPaulo"
export KEY_ORG="DEXTER"
export KEY_EMAIL="root@dexter.com.br"
```

GERANDO CERTIFICADO

Use a sequência de comandos abaixo para gerar o certificado de autoridade:

 # source vars
 # ./clean-all
 # ./build-ca

Preencha as informações do certificado:
Country Name (2 letter code) [BR]:**BR**
State or Province Name (full name) [SP]:**SP**
Locality Name (eg, city) [SaoPaulo]:**SaoPaulo**
Organization Name (eg, company) [DEXTER]:**DEXTER**
Organizational Unit Name (eg, section) []:**DEXTER**
Common Name (eg, your name or your server's hostname) [DEXTER CA]:
Name []:
Email Address [root@dexter.com.br]:**root@dexter.com.br**

GERANDO CERTIFICADO

./build-key-server server
Generating a 2048 bit RSA private key
....+++
..........+++
writing new private key to 'server.key'

Country Name (2 letter code) [BR]:**BR**
State or Province Name (full name) [SP]:**SP**
Locality Name (eg, city) [SaoPaulo]:**SaoPaulo**
Organization Name (eg, company) [DEXTER]:**DEXTER**
Organizational Unit Name (eg, section) []:**DEXTER**
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [root@dexter.com.br]:**root@dexter.com.br**

GERANDO CERTIFICADO

Using configuration from /etc/openvpn/2.0/openssl.cnf
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'BR'
stateOrProvinceName :PRINTABLE:'SP'
localityName :PRINTABLE:'SaoPaulo'
organizationName :PRINTABLE:'DEXTER'
organizationalUnitName:PRINTABLE:'DEXTER'
commonName :PRINTABLE:'server'
emailAddress :IA5STRING:'root@dexter.com.br'
Certificate is to be certified until Jun 25 01:31:25 2021 GMT (3650 days)
Sign the certificate? [y/n]:**y**
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

GERANDO CERTIFICADO

Liste o conteúdo do subdiretório keys e verifique o arquivo de certificado do servidor (server.csr), o arquivo da chave do servidor (server.key) e o certificado auto assinado (server.crt).

Gerando parâmetros Diffie-Hellman

Os parâmetros Diffie-Hellman são utilizados para a troca das chaves criptografadas durante a execução do OpenVPN. Use o script abaixo para gerar os parâmetros:

 # ./build-dh

CONFIGURANDO O SERVIDOR

Liste o conteúdo do subdiretório keys e verifique o arquivo com os parâmetros Diffie-Hellman (dh2048.pem).

Configurando o servidor OpenVPN

Com os certificados e chaves gerados, abra o arquivo do servidor e adicione as opções abaixo:

 # vim /etc/openvpn/server.conf

CONFIGURANDO O SERVIDOR

 # vim /etc/openvpn/server.conf

```
dev tun
ifconfig 10.0.0.1 10.0.0.2
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
user nobody
group nogroup
tls-server
tls-auth chave 0
```

CONFIGURANDO O SERVIDOR

Continuação:

 # vim /etc/openvpn/server.conf

```
ca 2.0/keys/ca.crt
cert 2.0/keys/server.crt
key 2.0/keys/server.key
dh 2.0/keys/dh2048.pem
cipher DES-EDE3-CBC
```

CONFIGURANDO O CLIENTE

Ainda na máquina servidor crie a chave e o certificado para a máquina cliente, com o hostname da maquina cliente.

```
# cd /etc/openvpn/2.0
# ./build-key client
```

Country Name (2 letter code) [BR]:**BR**
State or Province Name (full name) [SP]:**SP**
Locality Name (eg, city) [SaoPaulo]:**SaoPaulo**
Organization Name (eg, company) [DEXTER]:**DEXTER**
Organizational Unit Name (eg, section) []:**DEXTER**
Common Name (eg, your name or your server's hostname) [client]:
Name []:
Email Address [root@dexter.com.br]:**root@dexter.com.br**

CONFIGURANDO O CLIENTE

```
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BR'
stateOrProvinceName   :PRINTABLE:'SP'
localityName          :PRINTABLE:'SaoPaulo'
organizationName      :PRINTABLE:'DEXTER'
organizationalUnitName:PRINTABLE:'DEXTER'
commonName            :PRINTABLE:'client'
emailAddress          :IA5STRING:'root@dexter.com.br'
Certificate is to be certified until Jun 25 01:51:26 2021 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

CONFIGURANDO O CLIENTE

Faça a copia dos arquivos abaixo via ssh para a máquina cliente.

 # cd /etc/openvpn/2.0/keys
 # scp client.key client.crt ca.crt root@IP_DO_CLIENTE:/etc/openvpn

CONFIGURANDO O CLIENTE

```
# vim /etc/openvpn/client.conf
dev tun
ifconfig 10.0.0.2 10.0.0.1
remote 192.168.200.1
port 5000
comp-lzo
verb 4
keepalive 10 120
persist-key
persist-tun
float
user nobody
group nogroup
ns-cert-type server
```

CONFIGURANDO O CLIENTE

Continuação:

 # vim /etc/openvpn/client.conf

```
tls-client
tls-auth chave 1
ca ca.crt
cert client.crt
key client.key
cipher DES-EDE3-CBC
```

CONFIGURANDO O CLIENTE

Descrição das novas opções utilizadas:

ns-cert-type → Indica que certificado foi assinado pelo servidor;

tls-client → Habilita conexão TLS, ajudando a bloquear ataques DoS e flooding na porta do OpenVPN.

No servidor:
 # /etc/init.d/openvpn start

Depos no cliente:
 # /etc/init.d/openvpn start

CHECANDO CONEXÃO

No servidor:
 # ifconfig

tun0 Link encap:Não Especificado Endereço de HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet end.: 10.0.0.1 P-a-P:10.0.0.2 Masc:255.255.255.255

No cliente:
 # ifconfig

tun0 Link encap:Não Especificado Endereço de HW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet end.: 10.0.0.2 P-a-P:10.0.0.1 Masc:255.255.255.255